CLAIMS

What is claimed is:

1. A computer-implemented method of determining enforcement security devices in a network topology, the method comprising:

identifying a source node and a destination node for traffic that is to be sent through the network topology;

programmatically identifying nodes in the network topology that are part of a path closure set for that source node and destination node; and

identifying each node in the path closure set that is a security device to result in creating and storing a list of one or more enforcement security devices.

2. A method as recited in Claim 1, further comprising implementing a security policy on security devices that are identified as nodes in the path closure set.

3. A method as recited in Claim 1, wherein programmatically identifying nodes in the network topology that are part of a path closure set includes locating each node in the network topology, and determining if each located node is part of at least one non-looping communication path extending between the source node and the destination node.

4. A method as recited in Claim 1, wherein

the step of programmatically identifying nodes in the network topology that are part of a path closure set includes locating a plurality of nodes in the network topology, and determining if each of the plurality of nodes is part of at least one non-looping communication path extending between the source node and the destination node; and the step of identifying each node in the path closure set is performed so that a duration for identifying all nodes in the path closure set is proportional to a number of links between each node in the network topology.

5. A method as recited in Claim 1, wherein programmatically identifying nodes in the network topology that are part of a path closure set includes forward traversing a series of nodes sequentially before identifying all non-looping communication paths extending between the source node and the destination node, and determining if each node in the network topology satisfies at least one criteria for belonging to one of the non-looping communication paths identified as extending between the source node and the destination node.

6. A method as recited in Claim 1, wherein

programmatically identifying nodes in the network topology that are part of a path closure set includes determining, prior to identifying all of the nodes in the path closure set, if each node in the network topology satisfies at least one criteria for belonging in the path closure set, and

determining if each node in the network topology satisfies at least one criteria for belonging in the path closure set includes traversing amongst adjacent nodes in a sequence until each node in the network topology is checked to determine if that node satisfies the at least one criteria for belonging to the path closure set.

7. A method as recited in Claim 6, wherein determining if each node in the network topology satisfies at least one criteria for belonging in the path closure set includes at least one of (i) identifying that node as being in the path closure set if that node is part of a non-looping sequence of adjacent nodes that extend between the source node and the destination node, and (ii) identifying that node as being in the path closure set if that node is part of a looping sequence of nodes in which at least one node in the looping sequence is already designated as being part of the path closure set, and in which the at least one node designated as being part of the path closure set is not also a loop closure node for that looping sequence.

8. A method as recited in Claim 6, wherein determining if each node in the network topology satisfies at least one criteria for belonging in the path closure set includes at least one of (i) identifying that node as being in the path closure set if that node is part of a non-looping sequence of adjacent nodes that extend between the source node and the destination node, (ii) identifying that node as being in the path closure set if that node is part of a looping sequence of nodes in which at least one node in the looping sequence is already designated as being part of the path closure set, and in which the at least one node designated as being part of the path closure set is not also a loop closure node for that looping sequence, and (iii) identifying that node as being in the path closure set if that node is part of a looping sequence of nodes in which at least a first adjacent node to a loop closure node for that looping sequence of nodes is subsequently identified as being part of the path closure set.

9. A method as recited in Claim 1, wherein programmatically identifying nodes in the network topology that are part of a path closure set includes checking each node in the network topology as being part of the path closure set by forward traversing from the source node to a sequence of nodes that are adjacent to one another until each node in the network topology is checked.

10. A method as recited in Claim 1, wherein identifying each node in the path closure set includes checking each node in the network topology as being part of the path closure set using a depth-first methodology.

11. A method of determining enforcement security devices in a network topology, the method comprising the computer-implemented steps of:

locating a plurality of adjacent nodes in a sequence, the plurality of adjacent nodes being between a source node and a destination node in the network topology, each located node in the sequence having at least two adjacent nodes, including a previous node in the sequence and a next node in the sequence, wherein for each located node in the plurality of adjacent nodes, the next node is different than the previous node;

for each located node in the sequence:

determining if the located node is the destination node, and if the located node is the destination node, then identifying each node in the sequence as being part of a path closure set between the source node and the destination node;

determining if the located node is a loop closure node, and if the located node is a loop closure node, then determining if one or more nodes in the sequence that are part of a loop path defined by the loop closure node are already designated as being part of the path closure set, and

if one or more nodes in the sequence that are part of a loop path defined by the loop closure node are already designated as being part of the path closure set, then

designating each node in the loop path as part of the path closure set, else

designating each node in the loop path as part of the path closure set if at least a designated node in the loop path is subsequently determined to be part of the path closure set.

12. A method as recited in Claim 11, wherein locating a plurality of adjacent nodes in a sequence includes locating each node in the network topology using the sequence.

13. A method as recited by Claim 11, further comprising identifying one or more enforcement security devices from nodes in the path closure set.

14. A method as recited in Claim 11, further comprising identifying one or more enforcement security devices from nodes in the path closure set, and implementing a security policy on the identified one or more enforcement security devices.

15. A method as recited in Claim 11, determining that the located node is a loop closure node includes determining that the located node was located as a next node for at least two other nodes in the sequence.

16. A method as recited in Claim 11, wherein designating each node in the loop path as part of the path closure set if a designated node in the loop path is subsequently determined to be part of the path closure set includes designating each node in the loop path as part of the path closure set if one of the at least two nodes in the sequence that are adjacent to the loop closure node is subsequently determined to be part of the path closure set.

17. A method as recited in Claim 11, wherein locating a plurality of adjacent nodes in a sequence includes locating the plurality of nodes using a depth-first methodology.

18. A policy server communicatively coupled to one or more security devices in a network to implement a security policy, the policy server comprising:

a processor configured to:

identify a source node and a destination node for traffic that is to be sent through the network topology;

automatically identify nodes in the network topology that are part of a path closure set for that source node and destination node; and

identify each node in the path closure set that is a security device.

19. The policy server of claim 18, wherein the processor is configured to implement a security policy using the identified one or more enforcement security devices.

20. A computer readable medium for determining enforcement security devices in a network topology, the computer readable medium carrying instructions for performing the steps of:

identifying a source node and a destination node for traffic that is to be sent through the network topology;

programmatically identifying nodes in the network topology that are part of a path closure set for that source node and destination node; and

identifying each node in the path closure set that is a security device.

21. A computer readable medium as recited in Claim 20, further comprising instructions for implementing a security policy on security devices that are identified as nodes in the path closure set.

22. A computer readable medium as recited in Claim 20, wherein instructions for programmatically identifying nodes in the network topology that are part of a path closure set include instructions for locating each node in the network topology, and instructions for determining if the located node is part of at least one non-looping communication paths extending between the source node and the destination node.

23. A computer readable medium as recited in Claim 20, wherein

instructions for programmatically identifying nodes in the network topology that are part of a path closure set include instructions for locating a plurality of nodes in the network topology, and instructions for determining if the located node is part of at least one non-looping communication paths extending between the source node and the destination node; and

instructions for identifying each node in the path closure set is executed so that a duration for identifying each node in the path closure set is proportional to a number of links between each node in the network topology.

24. A computer readable medium as recited in Claim 20, wherein instructions for programmatically identifying nodes in the network topology that are part of a path closure set include instructions for forward traversing a series of nodes sequentially before identifying all non-looping communication paths extending between the source node and the destination node, and instructions for determining if each node in the network topology satisfies at least one criteria for belonging to one of the non-looping communication paths identified extending between the source node and the destination node.

25. A computer readable medium as recited in Claim 20, wherein

instructions for programmatically identifying nodes in the network topology that are part of a path closure set include instructions for determining, prior to identifying all of the nodes in the path closure set, if each node in the network topology satisfies at least one criteria for belonging in the path closure set, and

instructions for determining if each node in the network topology satisfies at least one criteria for belonging in the path closure set include instructions for traversing amongst adjacent nodes in a sequence until each node in the network topology is checked to determine if that node satisfies the at least one criteria for belonging to the path closure set.

26. A computer readable medium as recited in Claim 25, wherein instructions for determining if each node in the network topology satisfies at least one criteria for belonging in the path closure set includes instructions for at least one of (i) identifying that node as being in the path closure set if that node is part of a non-looping sequence of adjacent nodes that extend between the source node and the destination node, and (ii) identifying that node as being in the path closure set if that node is part of a looping sequence of nodes in which at least one node in the looping sequence is already designated as being part of the path closure set, and in which the at least one node designated as being part of the path closure set is not also a loop closure node for that looping sequence.

27. A computer readable medium as recited in Claim 25, wherein instructions for determining if each node in the network topology satisfies at least one criteria for belonging in the path closure set includes instructions for at least one of (i) identifying that node as being in the path closure set if that node is part of a non-looping sequence of adjacent nodes that extend between the source node and the destination node, and (ii) identifying that node as being in the path closure set if that node is part of a looping sequence of nodes in which at least one node in the looping sequence is already designated as being part of the path closure set, and in which the at least one node designated as being part of the path closure set is not also a loop closure node for that looping sequence (iii) identifying that node as being in the path closure set if that node is part of a looping sequence of nodes in which at least a first adjacent node to a loop closure node for that looping sequence of nodes is subsequently identified as being part of the path closure set.

28. A computer readable medium as recited in Claim 20, wherein instructions for programmatically identifying nodes in the network topology that are part of a path closure set includes instructions for checking each node in the network topology as being part of the path closure set by forward traversing from the source node to a series of nodes that are sequentially adjacent to one another until each node in the network topology is checked.

29. A computer readable medium as recited in Claim 20, wherein instructions for identifying each node in the path closure set includes instructions for checking each node in the network topology as being part of the path closure set using a depth-first methodology.

30. A computer system to determine enforcement security devices in a network topology:

a processor configured to:

means for identifying a source node and a destination node for traffic that is to be sent through the network topology;

means for automatically identifying nodes in the network topology that are part of a path closure set for that source node and destination node; and

means for identifying each node in the path closure set that is a security device.